Ben Barnow
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
Email: b.barnow@barnowlaw.com

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans Street, Suite 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

ATTORNEYS FOR STEVENS PLAINTIFFS
(additional counsel on signature page)

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

IN RE:

ZAPPOS.COM, INC. CUSTOMER DATA SECURITY BREACH LITIGATION

This Document Relates To:

3:12-cv-00339-RCJ-VPC (*Stevens*)
3:12-cv-00340-RCJ-VPC (*Penson*)
3:12-cv-00341-RCJ-VPC (*Elliott, Brown and Seal*) and Plaintiffs Denise Relethford and Emily E. Braxton

Case No. 3:12-cv-00325-RCJ-VPC
MDL No. 2357

STEVENS PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANT ZAPPOS.COM, INC.'s MOTION TO DISMISS SECOND AMENDED COMPLAINTS

Plaintiffs Theresa D. Stevens, Stacy Penson, Tara J. Elliot, Brooke C. Brown, Christa Seal, Denise Relethford, and Emily E. Braxton (collectively, "Stevens Plaintiffs" or "Plaintiffs"), through counsel, file this Response in Opposition to Defendant Zappos.com, Inc.'s ("Zappos") Motion to Dismiss Second Amended Complaints ("Motion to Dismiss" or "MTD") based on the following points and authorities:

POINTS AND AUTHORITIES

Zappos's unlawful, unfair, deceptive, and unconscionable conduct has caused Stevens Plaintiffs to suffer concrete and particularized harm and injuries—which is articulated in their well-pled Second Amended Consolidated Class Action Complaint ("SAC") [D.E. #119]. Zappos's MTD, therefore, should be denied for the following reasons.

I. Statement of Facts.

A. The Data Breach.

Plaintiffs and Class Members are consumers of shoes, apparel and other products sold by Zappos, an online retailer. SAC ¶1. As part of their transactions with Zappos, Plaintiffs and Class Members provided Zappos with their confidential personal customer account information, including, *inter alia*, their names, email addresses, billing and shipping addresses, phone numbers, the last four digits of their credit cards, and a Zappos.com website account password to make purchases from Zappos (collectively, "PCAI"). SAC ¶1. By providing this information to Zappos, Plaintiffs and Class Members entrusted Zappos with their PCAI and relied on Zappos to properly and adequately store and protect their PCAI. *Id.*

On, or prior to, January 15, 2012, Zappos servers in Kentucky and Nevada containing Plaintiffs' and Class Members' PCAI were improperly accessed without authorization (the "Data Breach"). SAC ¶2. Zappos failed to properly safeguard and protect the servers and failed to safeguard and protect Plaintiffs' and Class Members' PCAI accessed and taken by unauthorized third parties (*i.e.*, the Data Breach). *Id.*

On January 16, 2012, Zappos sent Plaintiffs and each Class Member an email notifying them its servers had been breached and their PCAI had been stolen and compromised. SAC ¶3. Tony Hsieh, Zappos's CEO, stated that Plaintiffs' and Class Members' PCAI was stolen by hackers who gained

access to Zappos's internal network through its unprotected servers. SAC ¶28. Zappos closed its customer service telephone lines for the week immediately following the Data Breach, depriving Plaintiffs and Class Members of the ability to find out more information about the Data Breach from Zappos, and preventing them from taking appropriate steps to prevent identify theft and/or fraud. SAC ¶¶3, 30.

Zappos disregarded Plaintiffs' and Class Members' privacy rights by failing to take the precautions required to safeguard and protect Plaintiffs' and Class Members' PCAI from unauthorized disclosure. SAC ¶¶4, 29. Zappos improperly handled and stored Plaintiffs' and Class Members' PCAI (which was private and sensitive information), did not encrypt or improperly partially encrypted their PCAI, inadequately protected their PCAI, made their PCAI readily accessible to data thieves, and failed to handle and store their PCAI in compliance with proper security protocols and standard industry practices "for protecting consumer financial data and personal identification information." SAC ¶¶4, 29.

B. Zappos's policies and representations regarding Plaintiffs' and Class Members' PCAI.

On Zappos's websites, Zappos.com and 6pm.com, Zappos's customers, including Plaintiffs and Class Members, were required to create accounts to purchase shoes, apparel and other products. SAC ¶22. In creating these accounts, Plaintiffs and Class Members provide Zappos with their PCAI—including, *inter alia*, their names, account numbers, passwords, e-mail addresses, billing and shipping addresses, phone numbers, and the last four digits of the credit cards used to make purchases. Each customer account is accessed by using a unique username and password. SAC ¶22.

In its "Privacy Policy," Zappos represents that "[a]ccess to your personal information is restricted. Only employees who need access to your personal information to perform a specific job are granted access to your personal information." SAC ¶23. Zappos also represents it "take[s] several steps to protect your personal information in our facilities," and "makes a 'Safe Shopping Guarantee,' promising that the use of credit card information on its websites is secure," in addition to "placing a yellow, lock-shaped icon on its website payment page that confirms entry of a consumer's PCAI as part of an online retail transaction with Zappos is safe and secure." SAC ¶¶23–25. Zappos's conduct, however, did not live up to its "Privacy Policy" and "Safe Shopping Guarantee," resulting

in the Data Breach and the wrongful disclosure of Plaintiffs' and Class Members' PCAI. SAC ¶26.

The Federal Trade Commission ("FTC") publication, "Protecting Personal Information: A Guide for Business," identifies how companies, such as Zappos, can guard against the theft of personal and sensitive information in their files, but Zappos is not known to have adopted these practices, as shown by the Data Breach. SAC ¶46.

C. The severity and impact of data breaches.

Javelin Strategy & Research's 2012 Identity Fraud Report ("the Javelin Report") quantifies the impact to consumers of data breaches. SAC ¶7. According to the Javelin Report, consumers "whose PCAI is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft." *Id.* Further, there is a strong likelihood that criminals who possess Plaintiffs' and Class Members' PCAI and have not yet used the information will do so at a later date, or even re-sell it. *Id.*

According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[1] SAC ¶33. "There is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device, even if the individual pieces of data do not constitute [PCAI]."[2] *Id.* Identity theft can take many forms, and it is not limited to the unauthorized use of credit cards. *See* SAC ¶¶38–41, 47.

D. Plaintiffs' claims and damages resulting from Zappos's Data Breach.

Zappos betrayed Plaintiffs' and Class Members' trust by failing to properly safeguard and protect their PCAI and publicly disclosing their PCAI without authorization. Plaintiffs sue Zappos for

---

[1] *Protecting Consumer Privacy in an Era of Rapid Change, FTC Report* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

[2] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, 35–38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11–12. An estimated 9 million American identities are stolen each year. *Id.*; SAC ¶34.

negligent misrepresentation, violation of various state deceptive trade practice acts or consumer protection acts, violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200 *et seq.* ("UCL"), violation of the security requirements for consumer records under Cal. Bus. & Prof. Code §§1798.29, 1798.80, *et seq.*, violation of the Consumer Legal Remedies Act, Cal. Civ. Code §1750 *et seq.* ("CLRA"), violation of the Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. & Com. Code §17.50(a)(3) ("TDTPA"), and unjust enrichment. SAC ¶¶71–143.

As a direct and/or proximate result of Zappos's actions and/or inactions and the resulting Data Breach, Plaintiffs and Class Members have incurred (and will continue to incur) the following concrete and particularized forms of cognizable harm and damages:

> (i) untimely and/or inadequate notification of the Data Breach, (ii) improper disclosure of their PCAI, (iii) closure of Zappos's customer service telephone lines, (iv) loss of the unencumbered use of their extant passwords and the loss of their passwords, (v) the oppressive Zappos.com website arbitration clause and Zappos's attempted enforcement of same, (vi) loss of privacy, (vii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach, (viii) the value of their time spent mitigating the increased risk of identity theft and/or identity fraud including, *inter alia*, changing their Zappos.com account passwords and passwords for other accounts using the same passwords, (ix) deprivation of the value of their PCAI, for which there is a well-established national and international market, (x) receipt of a diminished value of the services they paid Zappos to provide (*e.g.*, protection of their PCAI), and (xi) loss of the customer service access that was part of the services provided for by Zappos, and which was willfully severed by Zappos at a time of high need by its customers—for which they are entitled to compensation.

SAC ¶¶ 6, 44, 86, 97, 113, 122, 129, 136, and 145 [D.E. #119]. Zappos's wrongful conduct and the resulting Data Breach have also placed Plaintiffs and Class Members "at an imminent, immediate and continuing increased risk of identity theft and/or identity fraud," including a risk greater than in the absence of Zappos's misconduct. SAC ¶¶7, 31. Examples of these increased risks of identity theft and other losses include usage of and interference with their computers and other electronic devices, including smartphones, battery usage, space/capacity usage, service provider charges and similar issues, resulting from "phishing" and "pharming" related to the PCAI made available by Zappos. SAC ¶¶31, 35–37.

Plaintiffs and Class Members were also required to spend (and spent) time changing their Zappos.com account passwords (as recommended by Zappos and reasonable conduct), changing

their passwords "on any other web site where [Plaintiffs and Class Members] use the same or a similar password" (as further recommended by Zappos and reasonable conduct), and changing other portions of their already-compromised PCAI. SAC ¶31. Other than these recommendations, Zappos has not offered Plaintiffs and Class Members any compensation or protection from the Data Breach, such as credit monitoring services and/or identity theft insurance. SAC ¶45. At the same time, Plaintiffs' and Class Members' account passwords can sell for as much as $20 each on the black market.[3]

E. The Court's Order granting in part, and denying in part, Zappos's first motion to dismiss.

On September 9, 2013, the Court entered its Order granting in part, and denying in part, Zappos's first motion to dismiss (the "Order") [D.E. #114]. In its Order, the Court held that "[a]s a general matter, the Court finds that Plaintiffs have standing," and "standing is otherwise sufficiently alleged." *Id.* at 5. While the Court dismissed some of Plaintiffs' claims, the Court upheld Plaintiffs' claim for violation of Tex. Bus. & Com. Code § 17.50(a)(3)—along with Preira Plaintiffs' California consumer fraud law and data breach notice violations (the same as Plaintiffs' California claims in their SAC)—and allowed Plaintiffs leave to amend their negligence, unjust enrichment, and certain state consumer fraud claims. *Id.* at 5–13. Plaintiffs subsequently filed their SAC, which has engendered Zappos's second MTD.

ARGUMENT

I. Legal Standards on a Motion to Dismiss.

Zappos challenges Plaintiffs' SAC on two grounds: (i) Plaintiffs lack standing, and (ii) Plaintiffs fail to state a claim.

Plaintiffs have standing to assert their claims, as set forth in greater detail below. Plaintiffs also properly state their claims, as set forth on greater detail below—particularly because a plaintiff need

---

[3] N. Perlroth, *Twitter Hacked: Data for 250,000 Users May Be Stolen*, NYTimes (Feb. 1, 2013), *available at* http://bits.blogs.nytimes.com/2013/02/01/twitter-hacked-data-for-250000-users-stolen/?partner=rss&emc=rss&smid=tw-nytimes (last visited Dec. 18, 2013).

only plead "enough facts to state a claim to relief that is plausible on its face" and to "nudge[ ] [his or her] claims across the line from conceivable to plausible." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). The complaint must plead facts that are more than "'merely consistent with' a defendant's liability;" "the plaintiff [must] plead[ ] factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009).

A court must also accept as true all of the allegations in a complaint and give the plaintiff the benefit of all reasonable inferences from those allegations. *Clegg v. Cult Awareness Network*, 18 F.3d 752, 754 (9th Cir. 1994). "A complaint should not be dismissed unless it appears beyond doubt the plaintiff can prove no set of facts in support of his claim that would entitle him to relief." *Id.* "[D]ismissal is appropriate only when the complaint does not give the defendant fair notice of a legally cognizable claim and the grounds on which it rests." *Uranga v. Adams*, No. 3:10-CV-00014-RCJ, 2011 WL 147909, at *1 (D. Nev. Jan. 14, 2011). This determination is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." *Iqbal*, 129 S. Ct. at 1949.

Drawing upon the law, common sense, and experience, Plaintiffs' SAC meets the Rule 12(b)(6) pleading standard.

II. Plaintiffs Have Standing to Sue.

A. Plaintiffs have Article III standing.

Notwithstanding the Court's previous finding that Plaintiffs have standing to sue (Order at 5 [D.E. #114]), Zappos goes to the well and again raises the issue. Plaintiffs—once again—address Zappos's standing arguments, respectfully asserting they have Article III standing for the following reasons.

First (and foremost), Plaintiffs allege the following concrete and particularized forms of cognizable harm and damages directly and proximately caused by Zappos's wrongful actions and inactions and the resulting Data Breach they and Class Members have incurred (and will continue to incur)—all of which confer standing:

(i) untimely and/or inadequate notification of the Data Breach, (ii) improper

> disclosure of their PCAI, (iii) closure of Zappos' customer service telephone lines, (iv) loss of the unencumbered use of their extant passwords and the loos of their passwords, (v) the oppressive Zappos.com website arbitration clause and Zappos' attempted enforcement of same, (vi) loss of privacy, (vii) *out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach*, (viii) the value of their time spent mitigating the increased risk of identity theft and/or identity fraud including, *inter alia*, changing their Zappos.com account passwords and passwords for other accounts using the same passwords, (ix) deprivation of the value of their PCAI, for which there is a well-established national and international market, (x) receipt of a diminished value of the services they paid Zappos to provide (*e.g.*, protection of their PCAI), and (xi) loss of the customer service access that was part of the services provided for by Zappos.

SAC ¶¶6, 44, 86, 97, 113, 122, 129, 136, 145 (emphasis added). Faced with Plaintiffs' concise allegations, however, Zappos unashamedly argues they do not have standing because "Plaintiffs specifically do not allege that they incurred any out-of-pocket expenses on fraud prevention measures," "such as credit monitoring or other fraud prevention services." MTD at 12. Zappos is wrong. Setting aside the other ten tangible and cognizable forms of harm Plaintiffs and Class Members suffered—all of which confer standing—Zappos's standing argument should be rejected (again) for this reason alone.

Next, Zappos argues the applicability of *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013) (MTD at 11; 13-16), reprimanding the Court for not addressing *Clapper* in its previous Order. MTD at 12. In its arrogance, Zappos refuses to accept that the Court considered *Clapper* and rejected *Clapper* in finding Plaintiffs have standing to sue. In any event, a close review of *Clapper* confirms it supports Plaintiffs' Article III standing here.

In *Clapper*, plaintiffs challenged the constitutionality of the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA"), and the Foreign Intelligence Surveillance Courts ("FISC"). *Id.* at 1144. In *Clapper*, plaintiffs alleged that "there is an objectively reasonable likelihood that their communications will be acquired under [FISA]." *Id.* at 1146. Because the constitutionality of powers exercised by the other two government branches in the fields of intelligence gathering and foreign affairs were at issue, the court applied an "especially rigorous" standing inquiry. *Id.* at 1147.

Before addressing *Clapper* plaintiffs' claims, the Court noted it had "repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact' and that '[a]llegations of

possible future injury' are not sufficient," signifying that the Court was not making new law. *Id.* (citing *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (emphasis added to original by the *Clapper* Court)). The Court further held its "cases do not uniformly require plaintiffs to demonstrate it is literally certain that the harms they identify will come about. Sometimes, [the Court has] found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm." *Id.* at n.5 (collecting cases).

In concluding plaintiffs lacked Article III standing, the Court, in *Clapper*, noted it was "speculative" whether the government would actually acquire the plaintiffs' communications under FISA, and found that plaintiffs failed to set forth facts their communications would be targeted by the government. *Id.* at 1148–49. "In sum, [plaintiffs'] speculative chain of possibilities does not establish that injury based on potential future surveillance is certainly impending . . . ." *Id.* at 1150.

Here, on the other hand, there is no speculation about Plaintiffs' PCAI. Zappos has readily admitted this fact by notifying Plaintiffs and Class Members their PCAI was stolen and compromised in the Data Breach. These data thieves risked imprisonment to obtain this treasure trove of data. Zappos's hypothetical and far-flung "chain of events" that must occur for Plaintiffs to allegedly have Article III standing is not reality and should be disregarded.

Zappos recognizes the distinction between *Clapper* and this case. Zappos correctly states the *Clapper* plaintiffs asserted a standing theory based on "'an objectively reasonable likelihood that their communications *[would be] acquired* under § 1881a *at some point in the future*.'" MTD at 13 (quoting *Clapper*, 133 S. Ct. at 1143) (emphasis added). Yet, Zappos does not—and cannot—deny the reality that Plaintiffs' PCAI here already been stolen and compromised.

Further, because *Clapper* does not change Article III standing law, *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) remains in force in this Circuit. Importantly, *Krottner* does not require an actual instance of attempted identity theft:

> *Plaintiffs–Appellants have alleged a credible threat of real and immediate harm* stemming from the theft of a laptop containing their unencrypted personal data. Were Plaintiffs–Appellants' allegations more conjectural or hypothetical—for example, if no laptop had been stolen, and Plaintiffs had sued based on the risk that it would be stolen at some point in the future—we would find the threat far less credible. On these facts, however, Plaintiffs–Appellants have sufficiently alleged an injury-in-fact for purposes of Article III standing.

Krottner, 628 F.3d at 1143 (emphasis added). In any event, Plaintiffs allege far more than the increased risk of identity theft or identity fraud as the basis for their Data Breach damages. *See* SAC ¶¶6, 44, 86, 97, 113, 122, 129, 136, 145.

The value of Plaintiffs' PCAI is substantial. Consumers place a high value on their PCAI, as well as the *privacy* of such data. Studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49–44.62."[4] When consumers were surveyed about how much they value their personal data for its protection against improper access and unauthorized secondary use—two concerns at issue here—they valued the restriction of improper access at between $11.33 and $16.58 per website, and prohibiting secondary use at between $7.98 and $11.68 per website.[5] The value of Plaintiffs' PCAI on the black market is substantial—credit card numbers, for example, bring $1.50 to $90 per card number,[6] and passwords can command up to $20 each.[7] Zappos has deprived Plaintiffs of this value through its wrongful conduct.

Plaintiffs' allegations establish their injury is not just "certainly impending"—it has already occurred and continues. Zappos's attempt to wrap this case in different facts, circumstances, and risk to Plaintiffs and Class Members does not change either reality or the applicable law. Plaintiffs have standing to assert their claims under both *Krottner* and *Clapper*.

---

[4] Il-Horn Hann *et al.*, *The Value of Online Information Privacy: An Empirical Investigation* (Oct. 2002), available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (emphasis added) (last visited Dec. 27, 2013.

[5] *Id.*

[6] *The Cyber Black Market: What's Your Bank Login Worth*, available at http://www.ribbit.net/frogtalk/id/50/the-cyber-black-market-whats-your-bank-login-worth (last visited Dec. 27, 2013); Office of the National Counterintelligence Executive, *How Much Do You Cost on the Black Market*, available at http://www.ncix.gov/issues/cyber/identity_theft.php (last visited Dec. 27 2013).

[7] Nicole Perlroth, *Twitter Hacked: Data for 250,000 Users May Be Stolen*, The New York Times (Feb. 1, 2013), available at http://bits.blogs.nytimes.com/2013/02/01/twitter-hacked-data-for-250000-users-stolen/?smid=tw-share (last visited Dec. 27, 2013).

Finally, Zappos argues Plaintiffs do not have standing under the court's analysis in *In re Barnes & Noble PIN Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. September 3, 2013). MTD at 15–16. Setting aside the fact that *Krottner* remains in force in this Circuit, *Barnes & Noble* is easily distinguishable. For example, the *Barnes & Noble* plaintiffs did not plead "any facts to support the conclusion that their information was disclosed" to or "stolen" by the hackers—a critical missing allegation underpinning all of their claimed injuries. 2013 WL 4759588, at *4. Here, on the other hand, it is undisputed that Plaintiffs' and Class Members' PCAI was stolen and compromised in the Data Breach—as evidenced by the Data Breach email notifications Zappos ultimately sent.

The *Barnes & Noble* court also disregarded plaintiffs' standing argument based on the deprivation of the value of their personal information because they did not allege their personal information was sold or even could be sold for value. *Id.* at *5 (citations omitted). That certainly is not the case here. *See* SAC ¶¶ 6, 44, 48–55 (and accompanying footnotes), 86, 97, 113, 122, 129, 136, 145 ("deprivation of the value of their PCAI, for which there is a well-established national and international market"). Plaintiffs have Article III standing to sue.

B. Plaintiffs have standing under the CLRA.

Zappos also contends Plaintiffs do not have standing under the CLRA because they do not allege actual harm. MTD at 19–20. Zappos is mistaken about standing under the CLRA.

To have standing under the CLRA, a plaintiff must have "suffer[ed] any damages as a result of the . . . practice declared to be unlawful[.]" Cal. Civ. Code § 1780(a). "[T]he CLRA's 'any damage' requirement is a capacious one that includes any pecuniary damages as well as opportunity costs and transaction costs that result when a consumer is misled by deceptive marketing practices." *Hinojos v. Kohl's Corp.*, 718 F.3d 1098, 1108 (9th Cir. 2013) (quoting *Meyer v. Sprint Spectrum L.P.*, 45 Cal. 4th 634, 640 (Cal. 2009)); *see also Doe 1 v. AOL, LLC*, 719 F. Supp. 2d 1102, 1111–12 (N.D. Cal. 2010) (finding plaintiffs satisfied "any damage" requirement under the CLRA where they alleged that "[i]n contravention to its representations regarding maintaining the privacy of its members, [defendant] disclosed highly sensitive personal information").

Here, Plaintiffs allege they purchased shoes, apparel, and other goods from Zappos with the reasonable expectation that the PCAI they were required to provide to Zappos to complete their

transactions "would be safeguarded and protected by Zappos," when it was not. SAC ¶128. Plaintiffs allege that as a result of Zappos's wrongful conduct, Plaintiffs and Class Members were damaged because their PCAI was not maintained as promised (¶¶19, 129), they have had to mitigate the increased risk of identity theft, including resetting multiple passwords, and they have lost the value of their PCAI. SAC ¶129; *see also* ¶¶31, 47, 48. These damages fall within the broad range of "any damage" under the CLRA. *See Doe 1*, 719 F. Supp. 2d at 1111–12.

Zappos cites *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 965 (S.D. Cal. 2012)—but it is inapposite. There, the plaintiffs alleged that a data breach resulted in losing use of their network services and PlayStation consoles. Here, on the other hand, Plaintiffs allege they did not receive the benefit of their bargains because they paid for goods online with money and their PCAI on the condition their PCAI would be adequately maintained, and it was not. Plaintiffs, therefore, also have standing under the CLRA.

III. Plaintiffs May Pursue Claims Under Non-Nevada Statutes.

Zappos asserts that Nevada choice of law principles—and, therefore, Nevada law—apply to all of Plaintiffs' claims, precluding any claims under statutes of other states. MTD at 20. Plaintiffs concede that Nevada law applies to some of their claims because the laws of each jurisdiction compared to Nevada are fundamentally the same; to wit, negligent misrepresentation (Count I), violation of state deceptive trade practices and/or consumer protection acts (Count II); and unjust enrichment (Count VII). Regarding Plaintiffs' California claims,[8] Nevada choice of law principles apply because the claims arise from the SAC.

On the other hand, regarding Plaintiffs' claim for violation of the unconscionability prong of the

---

[8] Plaintiffs previously argued California choice of law principles apply to the California law claims asserted by Plaintiffs Relethford and Braxton because they originally filed their case in the Southern District of California before it was transferred by the MDL Panel to the District of Nevada. However, Plaintiffs Relethford and Braxton filed a Stipulation to Voluntarily Dismiss Without Prejudice Pursuant to F.R.C.P. 41(a)(1)(A)(ii) their pending complaint in this District. *See* Case No. 2:12-CV-00864-RCJ-PAL [D.E. #18]. The voluntary dismissal was filed "solely for the purpose of joining Plaintiffs and their claims within the amended complaint being filed in *In re Zappos.com, Inc., Customer Data Security Litigation*, Civil No. 3:12-cv-00325-RCJ-VPC, MDL No. 2357 (D. Nev.)." *Id.* Thus, Nevada choice of law principles now apply to their claims.

Texas Deceptive Trade Practices-Consumer Protection Act ("TDTPA") (Count VI), under a proper analysis of the actions transferred from Kentucky (*Stevens*, *Penson*, and *Elliot*), Kentucky choice of law rules must apply.

Both Nevada and Kentucky choice of law principles use the most significant relationship (or contacts) test and consider the following principles:

> (a) the needs of the interstate and international systems, (b) the relevant policies of the forum, (c) the relevant policies of other interested states and the relative interests of those states in the determination of the particular issue, (d) the protection of justified expectations, (e) the basic policies underlying the particular field of law, (f) certainty, predictability and uniformity of result, and (g) ease in the determination and application of the law to be applied.

RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6 (1971) (hereafter, the "most significant contacts test"). A proper analysis under the most significant contacts test confirms that Plaintiffs' California and Texas claims are properly pled.

A. Kentucky choice-of-law principles apply to Plaintiffs' TDTPA claim.

The Court previously held that Plaintiffs properly state a claim that Zappos violated the unconscionability prong of the TDTPA, section 17.50(a)(3). Order at 12 ("Plaintiffs have sufficiently alleged false, misleading, or deceptive practices via the statements on Zappos's website that Plaintiffs' personal data was secure. The Court will not dismiss this claim.") [D.E. #114].[9] Nevertheless, Zappos has "renew[ed]" its choice of law argument because, according to Zappos, "the Rule 12 Order does not address Zappos's choice-of-law argument made in connection with the original motion to dismiss." MTD at 20 n.11.

Once again, Zappos apparently cannot get its head around the fact that the Court considered the choice-of-law argument advanced by Zappos in its original motion to dismiss and rejected it, so—

---

[9] Zappos erroneously states the Court dismissed (without leave to amend) both of Plaintiffs' claims alleging Zappos violated the TDTPA. MTD at 7. The more accurate statement is the Court dismissed Plaintiffs' claim under Section 17.41 of the TDTPA (without leave to amend) "because any such amended claims would be duplicative with the claims under section 17.50 that are separately pled under the tenth cause of action, *infra*." Order at 12. Thus, the Court upheld Plaintiffs' claim under section 17.50 of the TDTPA (Count X in the CAC, which is now Count VI in the SAC). *Id.*

once again—Plaintiffs must respond.

The MDL Panel transferred three of Plaintiffs' cases from the Western District of Kentucky. These cases assert Alabama, Florida and Texas claims. As previously explained in Plaintiffs' response in opposition to Defendant's first motion to dismiss (D.E. #86 at 8–12), the Court, as the transferee court, must analyze Kentucky choice-of-law principles to determine which law the Kentucky court would have applied to Plaintiffs' claims filed in the Western District of Kentucky.[10]

Kentucky case law confirms that the RESTATEMENT'S "most significant contacts" test applies to contract and consumer protection act claims.[11] Applying the analysis advanced by the court in *In re Sigg Switzerland (USA)*—a factually similar situation—the Texas plaintiff (Plaintiff Stevens), who purchased goods from Zappos, has a claim under the TDTPA because Texas has a significant interest in protecting its residents as consumers and purchasers. 2011 WL 64289, at *6. Thus, Zappos "could reasonably expect to be held to the standards of the states in which they sell their [goods], and [Nevada's] interest in regulating its corporate residents does not override a state's interest in protecting its citizens. Once again, the law of the state of Plaintiffs' residence would apply." *Id.*

Plaintiffs' claim for violation of §17.50(a)(3) of the TDTPA (Count VI) falls under the *In re Sigg*

---

[10] *See, e.g., In re Sigg Switzerland (USA), Inc. Aluminum Bottles Marketing & Sales Prac. Litig.*, No. 10-MD-2137, 2011 WL 64289 (W.D. Ky. Jan. 7, 2011), wherein the court concluded that:

> [F]iling . . . the consolidated complaint did not waive any advantages that Plaintiffs retained based on their original forum selections. The consolidated complaint was largely filed for the organizational benefit of the Court and the parties. It did not seek to change any of the substantive claims of the parties or the applicable law, as evidenced by the consolidated complaint's retention of numerous state law claims based on different states' laws.
>
> These actions were originally filed in Kentucky, Minnesota and California. Given the above analysis, each of those states' choice-of-law provisions will apply to the claims filed in those states. *See Klaxon Co. v. Stentor Elec. Mfg. Co.*, 313 U.S. 487, 496–97 (1941).

2011 WL 64289, at *4.

[11] *See, e.g., In re Sigg*, 2011 WL 64289, at *4–*7; *Saleba v. Strand*, 300 S.W.3d 177, 181 (Ky. 2009) (citing Restatement (Second) of Conflict of Laws § 188 (1971); *Bonnlander v. Leader Nat. Ins. Co.*, 949 S.W.2d 618, 620 (Ky. Ct. App. 1996) (in tort actions, "any significant contact with Kentucky [i]s sufficient to allow Kentucky law to be applied," whereas in contract actions, "the law of the state with the greatest interest in the outcome of the litigation should be applied")).

Switzerland (USA) Kentucky choice-of-law analysis pertaining to consumer protection act claims. 2011 WL 64289, at *6. Count VI is a unique claim pled only on behalf of the Texas sub-class. Similar to the Texas plaintiff's claims in *In re Sigg Switzerland (USA)*, Plaintiff Stevens has a § 17.50(a)(3) unconscionability claim under the TDTPA because Texas "has a significant interest in the protection of its residents as consumers and purchasers." 2011 WL 64289, at *6.

While Zappos addresses the factors in the most significant contacts test, it fails to show that Nevada has the most significant relationship to the consumer protection claim brought by Plaintiff Stevens' claims under Texas law. The needs of interstate and international systems favors application of Texas law to claims of Texas residents who made their purchases in Texas and suffered injury from the Data Breach in Texas. Zappos argues that the policies of the forum favors Nevada law because "the injury at issue here is the alleged failure to adequately protect Plaintiffs' personal information and the resulting security breach," but Zappos misses the mark because it describes the conduct leading up to the injury—not the injury itself, which occurred in Texas.

Zappos also cites to a selection of Nevada law in its Terms of Use (MTD at 22); however, the Court has already found there was no agreement to Zappos's Terms of Use, and no contractual obligations were created by statements regarding the safety of customers' data. *See* D.E. #21 at 10 ("Where, as here, there is no acceptance by Plaintiffs, no meeting of the minds, and no manifestation of assent, there is no contract pursuant Nevada law."); D.E. #114 at 6 ("unilateral statements of fact alleged as to the safety of customers' data do not create any contractual obligations"). Thus, Zappos's argument that the parties would expect Nevada law to apply is misplaced. The TDTPA claim is only brought on behalf of the Texas sub-class, so Zappos is wrong to state that the Court will have to apply the laws of every state in this litigation. The TDTPA is properly pled.

B. Nevada choice-of-law principles apply to Plaintiffs' California claims.

Nevada uses the most significant contacts test in tort actions. *Gen. Motors Corp. v. Eighth Judicial Dist. Court of State of Nev. ex rel. Cnty. of Clark*, 122 Nev. 466, 474, 134 P.3d 111, 117 (Nev. 2006). Under this test, the factors or principles set forth above are considered but they "are not intended to be exclusive and no one principle is weighed more heavily than another." *Id*. Similar to the TDTPA claim, Zappos fails to show that Nevada has the most significant contacts to Plaintiffs'

California claims. Rather, Zappos merely cites to inapposite, mostly unpublished district court opinions without mentioning how they apply to the facts here.[12] MTD at 22–23. As one court noted in rejecting the application of Texas law to Californians, "[i]n light of California's materially greater interest in consumer protection issues related to its own citizens, . . . California law governs plaintiffs' statutory and common law claims." *Brazil v. Dell Inc.*, No. C-07-01700 RMW, 2010 WL 5387831, at *2 (N.D. Cal. Dec. 21, 2010)

The same concept also applies here. A California resident has a justified expectation that California law will apply to his or her claims because California-enacted statutes aim to protect their residents from injuries, such as those caused by the Zappos Data Breach. Plaintiffs' California claims in Counts III, IV, and V, therefore, are properly pled.

IV. Plaintiffs Properly State a Claim for Violation of the California Breach Notice Statute (Cal. Civ. Code § 1798.82, *et seq.*).

Zappos also moves to dismiss Plaintiffs' claim under the California Information Practices Act, Cal. Civ. Code §1798, *et seq.* ("California Breach Notice statute"). MTD at 16–20, 24–28. But, as noted above, the Court already upheld this very claim for Preira Plaintiffs. Order at 10–11 [D.E. #114]. It also should be upheld here. Zappos's second bite at the apple on this count should not be countenanced.

---

[12] *See Boise Tower Associates, LLC v. Washington Capital Joint Master Trust*, CV 03-141-S-MHW, 2006 WL 1749656 (D. Idaho June 22, 2006) (conducting an in-depth analysis under the most significant relationship test and finding that the state of Washington has the greatest interest in having its laws applied under plaintiff's tort of intentional interference of contract where most of the negotiations occurred in Washington); *Hycor Corp. v. Dontech, Inc.*, 84 C 3398, 1985 WL 3604 (N.D. Ill. Oct. 31, 1985) (Illinois law applied where the parties, the allegedly offensive bids, and injury all occurred in Illinois); *Abat v. Chase Bank USA, N.A.*, 738 F. Supp. 2d 1093, 1095 (C.D. Cal. 2010) (applying Delaware law pursuant to choice of law provision in parties' credit card agreements were the plaintiff was not a resident of California when she entered into the agreement); *Feld v. Am. Exp. Co.*, CV 09-7202-GW RCX, 2010 WL 9593386 (C.D. Cal. Jan. 25, 2010) (finding valid, bargained-for choice of law provision in parties' credit card agreements); *St. James v. Equilon Enterprises, LLC*, 08-CV-00962 W (AJB), 2008 WL 4279415 (S.D. Cal. Sept. 15, 2008) (enforcing choice of law provision where the plaintiff's claims can be afforded relief under Texas law in a manner that is not fundamentally different than under California law); *Tri-Cnty. Equip. & Leasing v. Klinke*, 286 P.3d 593, 595 (Nev. 2012) (applying forum law because there was no conflict of laws).

A. Plaintiffs suffered injury sufficient to assert California Breach Notice claims.

Zappos contends Plaintiffs lack Article III standing to sue under the California Breach Notice statute because, according to Zappos, Plaintiffs do not allege "concrete injury that results from their alleged failure to receive a notice that complied with the California law." MTD at 17. Zappos is wrong.

The Ninth Circuit has held that "[t]he injury required by Article III can exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" *Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010) (quoting *Fulfillment Servs. Inc. v. UPA*, 528 F.3d 614, 618 (9th Cir. 2008)); *see also Warth v. Seldin*, 422 U.S. 490, 500 (1975) ("[T]he actual or threatened injury required by [Article III] may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing . . . ."). Courts apply this principle to find Article III standing when a consumer alleges a violation of a consumer privacy statute with a private right of action.

In *Jewel v. N.S.A.*, 673 F.3d 902 (9th Cir. 2011), the plaintiff alleged violations of federal wiretapping laws. The court held that the plaintiff alleged a concrete and particularized injury because the wiretapping statute created a private right of action for violation of a statutory right. *Id.* at 908; *see also Graczyk v. West Publ'g Co.*, 660 F.3d 275, 277 (7th Cir. 2011) (injury established under Driver's Privacy Protection Act, which prohibits certain uses of information provided to DMVs); *Klimas v. Comcast Cable Commcn's, Inc.*, 465 F.3d 271, 275-76 (6th Cir. 2006) (privacy violation under the Cable Communications Policy Act constitutes standing even absent economic harm); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1055 (N.D. Cal. 2012) (alleged violations of Wiretap Act and the Stored Communications Act "serve as a concrete injury for the purpose of Article III injury analysis"); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 711–12 (N.D. Cal. 2011) (same).

The same is true here. By creating a specific civil enforcement mechanism for violations of the California Breach Notice statute, the California legislature has conferred standing on anyone who can plead and prove a statutory violation.

Claims under the California Breach Notice statute also are not limited to those who did not receive notice of the Data Breach because they cancelled their accounts or opted not to receive future

emails. *See* MTD at 18. Rather, the California Breach Notice statute requires that notice of a breach include the information in Section 1798.82(d) and be provided within "the most expedient time possible without unreasonable delay." Cal. Civ. Code § 1798.82(a); *see also id.* § 1798.29(a). The point here is that Plaintiffs do not allege they did not receive the email—as Zappos argues—but rather, Zappos's Data Breach email notice violated the California Breach Notice statute because it did not contain the requisite information and was not made without unreasonable delay. SAC ¶¶120, 122. In any event, whether the Zappos's Data Breach email notice was adequate and/or sent without unreasonable delay are questions of fact that cannot be resolved on a motion to dismiss.

B. "Personal Information" was compromised.

California Civil Code §1798.82(a) requires any person or business "that owns or licenses computerized data that includes personal information, shall disclose any breach of the surety of the system following discovery or notification of the breach . . . ." Here, Zappos contends it did not disclose "personal information" in violation of Section 1798.82(a) because only passwords and email addresses were stolen and compromised. MTD at 24.

But the California Breach Notice statute expressly states that "personal information" includes an individual's name together with an "[a]ccount number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." Cal. Civ. Code §1798.82(h)(3). Plaintiffs allege sufficient information was stolen to permit access to their financial accounts. Plaintiffs allege that names, email addresses, billing and shipping addresses, phone numbers, portions of credit card numbers, and passwords (*i.e.*, their PCAI) were stolen. SAC ¶¶1, 22. Plaintiffs specifically allege their names, in combination with their passwords, gives the cyber criminals access to their Zappos accounts containing saved credit card information and/or other personally identifying information that would allow access to financial accounts. SAC ¶¶32–43. Plaintiffs also allege that a criminal who has access to their email addresses, credit card numbers, and passwords can "phish" and "use the stolen information to clean out [a] victim's bank accounts or commit other forms of identity theft." SAC ¶35.

Plaintiffs' allegations are consistent with the California legislature's intent "to protect the privacy of individuals" by imposing "strict limits" on the "maintenance and dissemination of personal information." Cal. Civ. Code § 1798.1(c); *see also id.* § 1798.1(b) ("The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."). Nothing in the legislative history of the California Breach Notice statute submitted by Zappos requires anything more. The legislative history simply reveals that where only a person's username and password are stolen to allow access to a non-financial account, the California Breach Notice statute did not apply. *See* RJN, Ex. A at 9, 59, 64. Indeed, the revised bill specifically adds "an individual's username or email address, in combination with their password or security questions and answers" to the "personal information." *Id.* at 12, 61. Plaintiffs, however, allege much more than just the theft of their user names and passwords, including portions of their credit card numbers, which would permit access to their financial accounts. SAC ¶¶1, 22; *see also* ¶¶32–43.

V. Plaintiffs Properly Plead Their Unjust Enrichment Claim.

Plaintiffs state a valid claim for unjust enrichment under Nevada law and their respective home state laws, as all such laws are fundamentally similar in their requirements. Plaintiffs plainly allege (i) they conferred benefits on Zappos "in the form of their PCAI that Zappos . . . could use to track their buying habits and enaged in targeted marketing of specific shoes, apparel, and other goods that, in turn, increased Zappos's (and therefore Amazon.com's) revenues and profits," and because Plaintiffs' PCAI has "value on the robust domestic and internantional 'big data' market;" (ii) Zappos had knowledge of and retained these benefits; and (iii) under the circumstances—to wit, Zappos's failure to safeguard and protect Plaintiffs' PCAI—Zappos's retention of these substantial and commercial financial benefits is unjust. SAC ¶¶139–42; *see also, e.g., Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012); *Leasepartners Corp. v. Robert L. Brooks Trust Dated November 12, 1975*, 113 Nev. 747, 755, 942 P.2d 182, 187 (Nev. 1997); RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (2011) ("A person who is unjustly enriched at the expense of another is required to make restitution to the other.").

Zappos argues the above benefits have no value and no inequity exists here. MTD at 46. But, as

Zappos recognizes, Plaintiffs' allegations must be taken as true for purposes of a Rule 12(b)(6) motion to dismiss. Zappos's substantive arguments also fail. Zappos's practice of collecting consumers' PCAI allows it to increase its profits by targeting consumers with specific advertising and sales information tailored to each customer without otherwise compensating Plaintiffs and Class Members for their PCAI. SAC ¶¶139–41. Zappos does not dispute this indisputable fact.

Given the breach of its servers and the resulting Data Breach, it would be inequitable for Zappos to retain the benefits conferred on it by Plaintiffs and Class Members now that their PCAI has been released and they are subject to an increased risk of identity theft and/or fraud. Plaintiffs' unjust enrichment claim is properly pleaded. *See, e.g.*, *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 815 (N.D. Cal. 2011) (dismissing claim for unjust enrichment because no such claim existed under California law, but recognizing defendant's alleged conduct in using plaintiffs' personal information for its own financial gain qualified for restitution to plaintiffs); *Cain v. Redbox Automated Retail, LLC*, No. 2:12-CV-15014, 2013 WL 5977931, at *11 (E.D. Mich. Nov. 12, 2013) (upholding unjust enrichment claim where personal information was improperly disclosed, and holding that "this Court must take Plaintiffs' Complaint at its word").

CONCLUSION

Wherefore, Plaintiffs respectfully request that the Court deny Zappos's Motion to Dismiss, and grant them such other and further relief the Court deems just and appropriate.

Dated: December 27, 2013

Respectfully submitted,

By: /s/ Ben Barnow

Ben Barnow
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
b.barnow@barnowlaw.com

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans Street, Suite 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
rcoffman@coffmanlawfirm.com

Timothy G. Blood
BLOOD HURST & O'REARDON, LLP
701 B Street, Suite 1700
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101

Lance A. Harke, P.A.
HARKE CLASBY & BUSHMAN, LLP
9699 NE Second Avenue
Miami Shores, FL 33138
Telephone: (305) 536-8220
Facsimile: (305) 536-8229

E. Kirk Wood, Jr.
WOOD LAW FIRM, LLC
P.O. Box 382434
Birmingham, AL 35238-2434
Telephone: (205) 612-3905
Facsimile: (866) 747-3905

Mark K. Gray
GRAY & WHITE
713 East Market Street
Louisville, KY 40202
Telephone: (502) 210-8942
Facsimile: (502) 618-4059

ATTORNEYS FOR THE STEVENS PLAINTIFFS

CERTIFICATE OF SERVICE

On December 27, 2013, I caused the Stevens Plaintiffs' Response in Opposition to Defendant Zappos.com, Inc.'s Motion to Dismiss Second Amended Complaints to be electronically filed with the U.S.D.C., District of Nevada, using the CM/ECF system, which will automatically serve copies of the document on all registered CM/ECF users. For all non-ECF Users, service will be effectuated via First Class Mail.

/s/ Ben Barnow
Ben Barnow
BARNOW AND ASSOCIATES, P.C.
One North LaSalle Street, Suite 4600
Chicago, Illinois 60602
Telephone: (312)621-2000
Facsimile: (312) 641-5504
b.barnow@barnowlaw.com

ONE OF THE ATTORNEYS FOR THE STEVENS PLAINTIFFS